UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

In re: Conifer Data Security Breach Litigation	**Case No. 3:23-cv-00744-E-BN** **(Consolidated with 3:23-cv-870-E-BN)** **JURY TRIAL DEMANDED**

AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Nicole Kolb and William Tang ("Plaintiffs"), through their attorneys, individually and on behalf of all others similarly situated, bring this Class Action Complaint against Defendants Conifer Value-Based Care, LLC, Conifer Health Solutions, LLC, Conifer Revenue Cycle Solutions, LLC, and Tenet Healthcare Corporation ("Conifer" and with Tenet, "Defendants"), and their present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiffs allege the following on information and belief—except as to his own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendants' failure to protect highly sensitive data.

2. Defendant Conifer Value-Based Care, LLC is a Maryland LLC and subsidiary of parent Conifer Health Solutions, LLC, a Delaware LLC and it is a subsidiary of Tenet Healthcare Corporation whose headquarters and principal place of business is 14201 Dallas Pkwy., Dallas, Dallas County, Texas. Defendant Conifer Revenue Cycle Solutions, LLC is a California LLC and subsidiary of Conifer Health Solutions, LLC with its principal place of business in Texas. All three Conifer defendants are ultimately subsidiaries of Tenet Healthcare Corporation and on information and belief controlled by Tenet. All three Conifer defendants and Tenet share the same registered agent for service of process: CT Corporation, 1999 Bryan Street,

Ste. 900, Dallas, Texas 75201.

3. Defendant Conifer Health Solutions, LLC maintains its corporate headquarters in Texas. Among other things, Conifer's business provides revenue cycle management to healthcare providers. Upon information and belief this is done through its subsidiary Conifer Revenue Cycle Solutions, LLC.

4. Defendant Conifer Revenue Cycle Solutions, LLC, upon information and belief, provides revenue cycle management to its parent Conifer Health Solutions, LLC, and its customers.

5. Defendant Tenet Healthcare Corporation is the parent company for Defendant Conifer Health Solutions, LLC and maintains its corporate headquarters and principal place of business in Dallas, Texas. Conifer and its subsidiaries are some of Tenet's businesses, along with USPI (an ambulatory surgery platform) and Tenet's hospitals and physicians, among others.

6. Conifer provides hospitals and healthcare systems with "revenue cycle and value- based care solutions that optimize financial performance, improve business outcomes and elevate the healthcare experience."[1]

7. As part of the services Tenet and Conifer provide their customers, they store a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about their customers' current and former patients. But Tenet and Conifer lost control over that data when cybercriminals infiltrated their insufficiently protected computer systems in a data breach (the "Data Breach"). PII and PHI is collectively referred to as "Sensitive Information."

8. Defendants were unaware cybercriminals had accessed its network for nearly

[1] https://www.coniferhealth.com/

four months before the breach was discovered. In other words, Defendants had no effective means to prevent, detect, stop, or mitigate breaches of their systems—thereby allowing cybercriminals unrestricted access to patients' Sensitive Information.

9. On information and belief, cybercriminals were able to breach Defendants' systems because Defendants failed to adequately train their employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's Sensitive Information. In short, Defendants' failures placed the Class's Sensitive Information in a vulnerable position— rendering them easy targets for cybercriminals.

10. Plaintiffs are Data Breach victims, having received a legally required breach notice. They bring this class action on behalf of themselves, and all others harmed by Defendants' misconduct.

PARTIES

11. Plaintiff Nicole Kolb is a natural person and citizen of California. She resides in Los Angeles, California, where she intends to remain.

12. Plaintiff, William Tang, is a natural person and citizen of California. He resides in La Canada Flintridge, California, where he intends to remain.

13. Conifer Value-Based Care, LLC is a Maryland LLC with its registered agent being CT Corporation at 1999 Bryan Street, Suite 900, Dallas, Texas 75201. It can be served there. The sole member of Conifer Value-Based Care, LLC, is Conifer Health Solutions, LLC, a Delaware LLC. The members of Conifer Health Solutions, LLC are CommonSpirit Health and Conifer Holdings, Inc. CommonSpirit Health is a Colorado non-profit corporation with its principal place of business in Denver, Colorado. Conifer Holdings, Inc. is a Delaware corporation with its principal place of business in Frisco, Texas. Thus, Conifer Value-Based

Care, LLC is a citizen of Colorado, Delaware, and Texas.

14. Conifer Health Solutions, LLC, is a Delaware LLC with its principal place of business in Texas. Defendant Conifer Health Solutions, LLC can be served through its Registered Agent, CT Corporation System, 1999 Bryan St., Suite 900, Dallas, TX 75201. The members of Conifer Health Solutions, LLC, are CommonSpirit Health and Conifer Holdings, Inc. CommonSpirit Health is a Colorado non-profit corporation with its principal place of business in Denver, Colorado. Conifer Holdings, Inc. is a Delaware corporation with its principal place of business in Frisco, Texas. Thus, Conifer Health Solutions, LLC, is a citizen of Colorado, Delaware, and Texas.

15. Conifer Revenue Cycle Solutions, LLC is a California LLC that, according to the Texas Secretary of State, is located at 1445 Ross Ave., Suite 1400, Dallas, Texas 75202. It may be served with process through its registered agent, CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. The sole member of Conifer Revenue Cycle Solutions, LLC is Conifer Health Solutions, LLC. The members of Conifer Health Solutions, LLC are CommonSpirit Health and Conifer Holdings, Inc. CommonSpirit Health is a Colorado non-profit corporation with its principal place of business in Denver, Colorado. Conifer Holdings, Inc. is a Delaware corporation with its principal place of business in Frisco, Texas. Thus, Conifer Revenue Cycle Solutions, LLC is a citizen of Colorado, Delaware, and Texas.

16. Tenet Healthcare Corporation, the parent company of the Conifer defendants, is incorporated in Nevada and maintains its headquarters at 14201 Dallas Pkwy, Dallas, Texas, 75254. This is its principal place of business. Defendant Tenet Healthcare Corporation may be served through its Registered Agent, CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201. Tenet Healthcare Corporation is a citizen of Nevada and Texas.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The Plaintiffs are citizens of different states than each Defendant. And there are over 100 putative Class Members.

18. This Court has personal jurisdiction over Defendants because they are headquartered in Texas, regularly conduct business in Texas, and have sufficient minimum contacts in Texas.

19. Venue is proper in this Court because Tenet's principal place of business and headquarters are in the Dallas Division of the Northern District of Texas and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District. Tenet is the parent of the Conifer defendants.

BACKGROUND

Defendants Collected and Stored the Sensitive Information of Plaintiffs and the Class

20. Tenet, which wholly owns and operates Conifer as one of its three key business units, purports to be a "leading health system and services platform."[2] Tenet claims that Conifer is a key part of its business, focused on providing "the foundation for better health for clients across the country, through the delivery of healthcare-focused revenue cycle management and value- based care solutions."[3]

21. Defendants claim that Conifer is an "expert[] at the business of healthcare"[4] and

[2] https://www.tenethealth.com/about
[3] *Id.*
[4] *About*, CONIFER HEALTH SOLUTIONS, https://www.coniferhealth.com/about-us/ (last visited Mar. 13, 2023).

represents that what truly sets it apart is "how we deliver revenue cycle management and value-based care services."[5]

22. As part of its business, Conifer receives and maintains the Sensitive Information of thousands of third-party consumers, none of whom do any business directly with Conifer.

23. After collecting Sensitive Information from its customers, Defendants maintain the Sensitive Information on their computer systems. In obtaining and maintaining the Sensitive Information, Conifer and Tenet implicitly agreed it would safeguard the Sensitive Information of Plaintiffs and the Class in accordance with its internal policies, state law, and federal law.

24. Under state and federal law, businesses like Defendants have duties to protect its third-party consumers' Sensitive Information and to notify them about breaches.

25. In fact, Conifer represents on its Privacy Policy page on its website that "Your privacy is important to us and we want you to feel comfortable visiting the website of Conifer Health Solutions, LLC."[6] Conifer further represents that "While visiting our Site, if you provide personal information in order to receive information from us, such as to pre-register for a webinar, or for any other purpose, we will collect and store that data in an environment that employs industry standard security protections."[7]

Defendants' Data Breach

26. On January 20, 2022, Conifer was hacked—exposing the Sensitive Information of an unknown number of third-party consumers. Upon information and belief, these persons include the current and former patients of Conifer's customers.

27. The hack was not discovered until April 14, 2022, nearly four months later.[6]

[5] *Id.*
[6] https://www.coniferhealth.com/privacy-policy-2/.
[7] *Id.*
[6] *Notice of a Data Breach*, CONIFER HEALTH SOLUTIONS, attached as Exhibit A.

Conifer admits that "an unauthorized third party gained access to a Microsoft Office 365-hosted business email account."[7]

28. Defendants' Data Breach may have included one or more of the following types of Sensitive Information: full name, home address, date of birth, medical and treatment information, health insurance information, and billing and claims information.[8] Additionally, the social security number, driver's license number, and financial account information of some of the Class may have been impacted. At present this information is known only to the defendants.

29. Conifer and Tenet waited until August 12, 2022, nearly eight months after the Data Breach, to begin notifying its client healthcare providers, and then it took until September 30, 2022, until notification was made to Plaintiffs—now more than eight months after the Data Breach.[9]

30. Thus, Defendants kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

31. And when Defendants did notify Plaintiffs and the Class of the Data Breach, Defendants acknowledged that their Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and the Class to "review credit reports and statements sent from providers as well as your insurance company to ensure that all of your account activity is valid."[10]

32. Simply put, Defendants failed their duties when their inadequate security practices placed the Sensitive Information of Plaintiffs and Class Members into the hands of

[7] *Id.*
[8] *Id.*
[9] *Id.*

[10] *Id.*

cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs and Class Members.

33. Still, Conifer declares that it "takes privacy and security very seriously" and "sincerely regrets that this incident occurred and apologizes for any inconvenience this incident may have caused."[11] Regardless, Defendants' Data Breach caused widespread injury and monetary damages.

34. Since the breach, Conifer declared that it "continues to enhance its security controls and monitoring practices as appropriate to minimize the risk of any similar incident in the future…"[12] But this is too little too late. Simply put, these measures—which Conifer now recognizes as necessary—should have been implemented by Defendants *before* the Data Breach.

35. Defendants' negligence is evidenced by their failure to prevent the Data Breach and stop cybercriminals from accessing the Sensitive Information. And on information and belief, Defendants failed to adequately train their employees on reasonable cybersecurity protocols or implement reasonable security measures.

36. Defendants have offered nothing to Plaintiffs to attempt to remedy the ill effects Plaintiffs will suffer as a result of this Data Breach.

37. Moreover, it appears that another of Conifer's entities, Conifer Value-Based Care, LLC, experienced a separate data breach around the same time period as the Data Breach at issue here. Conifer Health Solutions provided notice that on March 21, 2022, it discovered that "an unauthorized third party gained access to certain Microsoft Office 365-hosted business email accounts through phishing" and was able to access Conifer Value-Based Care business

[11] *Id.*
[12] *Id.*

email accounts, which contained consumers' personal information[13].

38. Conifer Health Solutions reported that it provided notice to affected clients in August 2022 and that the breach involved individuals' names, addresses, dates of birth, health insurance information, medical information (including diagnosis and treatment information), and Social Security numbers[814].

39. The proximity of these two serious data breaches makes clear that Defendants were not adequately protecting the sensitive information it possessed.

Plaintiff Nicole Kolb's Experiences and Injuries

40. Plaintiff Nicole Kolb received Defendants' data breach notice on or about September 30, 2022. She is a former patient of one of Conifer's customers.

41. But no matter why Defendants possess Ms. Kolb's Sensitive Information, they have a duty to safeguard her information according to its internal policies and state and federal law.

42. Defendants deprived Ms. Kolb of the earlier opportunity to guard herself against the Data Breach's effects by failing to notify her for more than eight months.

43. Indeed, Ms. Kolb experienced an increase in spam texts and phone calls since the Data Breach, suggesting that her information has been placed in the hands of cybercriminals.

44. As a result of the Data Breach and the recommendation of Defendants' Notice, Ms. Kolb has spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been

[13] Ex. A
[14] *Id*

lost forever and cannot be recaptured.

45. Ms. Kolb has and will spend considerable time and effort monitoring her accounts to protect herself from identity theft. Ms. Kolb fears for her personal financial security and uncertainty over what Sensitive Information exposed in the Data Breach. Ms. Kolb has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

46. Plaintiff suffered actual injury from the exposure of her Sensitive Information — which violates her rights to privacy.

47. Ms. Kolb has suffered actual injury in the form of damages to and diminution in the value of her Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

48. Ms. Kolb has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her Sensitive Information being placed in the hands of unauthorized third parties and possibly criminals.

49. Ms. Kolb has a continuing interest in ensuring that her Sensitive Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff William Tang's Experiences and Injuries

50. Plaintiff William Tang received Defendants' data breach notice on or about September 30, 2022. He is a former patient of one of Conifer's customers.

51. But no matter why Defendants possess Plaintiff's Sensitive Information, they have

a duty to safeguard his information according to its internal policies and state and federal law.

52. Defendants deprived Plaintiff of the earlier opportunity to guard himself against the Data Breach's effects by failing to notify him for more than eight months.

53. Indeed, Plaintiff has experienced an increase in spam texts and phone calls since the Data Breach, suggesting that his information has been placed in the hands of cybercriminals.

54. As a result of the Data Breach and the recommendation of Defendants' Notice, Plaintiff has spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

55. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security and uncertainty over what Sensitive Information exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

56. Plaintiff suffered actual injury from the exposure of his Sensitive Information — which violates his rights to privacy.

57. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of his Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

58. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Sensitive

Information being placed in the hands of unauthorized third parties and possibly criminals.

59. Plaintiff has a continuing interest in ensuring that his Sensitive Information, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

60. Because of Defendants' failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. Loss of the opportunity to control how their Sensitive Information is used;

b. Diminution in value of their Sensitive Information;

c. Compromise and continuing publication of their Sensitive Information;

d. Out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. Lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of their stolen Sensitive Information; and

h. Continued risk to their Sensitive Information —which remains in Defendants' possession—and is thus at risk for futures breaches so long as Defendants fail to take appropriate measures to protect the Sensitive Information.

61. Stolen PII is one of the most valuable commodities on the criminal information

black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

62. The value of Plaintiffs' and Class's Sensitive Information on the black market is considerable. Stolen Sensitive Information trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "dark web"—further exposing the information.

63. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the Sensitive Information far and wide.

64. One way that criminals profit from stolen Sensitive Information is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen Sensitive Information, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

65. The development of "Fullz" packages means that the Sensitive Information exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

66. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Sensitive Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Sensitive Information is being misused, and that such misuse is fairly traceable to the

Data Breach.

67. Defendants disclosed the Sensitive Information of Plaintiffs and Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the Sensitive Information of Plaintiffs and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

68. Defendants' failure to promptly and properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendants Knew—Or Should Have Known—of the Risk of a Data Breach

69. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

70. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[15] Of the 1,862 recorded data breaches, 330 of them, or 17.7% were in the medical or healthcare industry.[16] Those 330 reported breaches exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[17]

71. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are

[15] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.
[16] *Id.*
[17] *Id.*

aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[18]

72. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[19]

73. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Defendants.

Defendants Failed to Follow FTC Guidelines

74. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendants—should use to protect against unlawful data exposure.

75. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[20] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

[18] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted- ransomware.
[19] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers- phishing-attack (last visited July 31, 2022).
[20] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting- personal-information.pdf.

76. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

77. Furthermore, the FTC explains that companies must:

a. Not maintain information longer than is needed to authorize a transaction;

b. Limit access to sensitive data;

c. Require complex passwords to be used on networks;

d. Use industry-tested methods for security;

e. Monitor for suspicious activity on the network; and

f. Verify that third-party service providers use reasonable security measures.

78. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

79. In short, Defendants' failure to use reasonable and appropriate measures to protect against unauthorized access to current and former patients' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendants Violated HIPAA

80. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic

transactions and code sets to maintain the privacy and security of protected health information.[21]

81. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[22]

82. The Data Breach itself resulted from a combination of inadequacies showing Defendants failed to comply with safeguards mandated by HIPAA. Defendants' security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendants' workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R.

[21] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[22] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards

§ 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

83. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

84. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

All individuals residing in the United States whose Personally Identifiable Information/Personal Health Information (PII/PHI) was compromised in the Data Breach discovered by Defendants in January 2022.

85. Excluded from the Class are Defendants, their agents, affiliates, parents,

subsidiaries, any entity in which Defendants have a controlling interest, any officer or director of Defendants, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

86. Plaintiffs reserve the right to amend the class definition.

87. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of his claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

88. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendants' custody and control. After all, Defendants already identified some individuals and sent them data breach notices.

89. Numerosity. Plaintiffs are representatives of the proposed Class, consisting of potentially thousands of members, far too many to join in a single action.

90. Commonality and Predominance. Plaintiffs and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. If Defendants had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's Sensitive Information;

b. If Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. If Defendants were negligent in maintaining, protecting, and securing Sensitive Information;

d. If Defendants took reasonable measures to determine the extent of the Data Breach after discovering it;

e. if Defendants' Breach Notice was reasonable;

f. if the Data Breach caused Plaintiffs and the Class injuries;

g. what the proper damages measure is; and

h. if Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief.

91. Typicality. Plaintiffs' claims are typical of Class member's claims as each arises from the same Data Breach, the same alleged violations by Defendants, and the same unreasonable manner of notifying individuals about the Data Breach.

92. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class members' interests. And Plaintiffs have retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

93. Superiority. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendants would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale,

provides comprehensive supervision by a single court, and presents no unusual management difficulties.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

94. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

95. Plaintiffs and members of the Class entrusted their Sensitive Information to Defendants and Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care in safeguarding and protecting their Sensitive Information and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendants' security systems to ensure the Sensitive Information of Plaintiffs and the Class was adequately secured and protected, including using encryption technologies. Defendants further had a duty to implement processes that would detect a breach of its security system in a timely manner.

96. Defendants were under a basic duty to act with reasonable care when it undertook to collect, create, and store Plaintiffs' and the Class's Sensitive Information on its computer system, fully aware–as any reasonable entity of its size would be–of the prevalence of data breaches and the resulting harm such a breach would cause. The recognition of Defendants duty to act reasonably in this context is consistent with, *inter alia*, the Restatement (Second) of Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

97. Defendants knew that the Sensitive Information of Plaintiffs and the Class was information that is valuable to identity thieves and other criminals. Defendants also knew of the

serious harms that could happen if the Sensitive Information of Plaintiffs and the Class was wrongfully disclosed.

98. By being entrusted by Plaintiffs and the Class to safeguard their Sensitive Information, Defendants had a special relationship with Plaintiffs and the Class. Plaintiffs' and the Class's Sensitive Information was provided to Defendants with the understanding that Defendants would take appropriate measures to protect it and would inform Plaintiffs and the Class of any security concerns that might call for action by Plaintiffs and the Class.

99. Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' Sensitive Information by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite failures and intrusions, and allowing unauthorized access to Plaintiffs' and the Class's Sensitive Information. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiffs and the Class, their Sensitive Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' negligence was a direct and legal cause of the theft of the Sensitive Information of Plaintiffs and the Class and all resulting damages. The injury and harm suffered by Plaintiffs and the Class members was the realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

100. Defendants knew that the Sensitive Information of Plaintiffs and the Class was information that is valuable to identity thieves and other criminals. Defendants also knew of the serious harms that could happen if the Sensitive Information of Plaintiffs and the Class was wrongfully disclosed.

101. By being entrusted by Plaintiffs and the Class to safeguard their Sensitive

Information, Defendants had a special relationship with Plaintiffs and the Class. Plaintiffs' and the Class's Sensitive Information was provided to Defendants with the understanding that Defendants would take appropriate measures to protect it and would inform Plaintiffs and the Class of any security concerns that might call for action by Plaintiffs and the Class.

102. Defendants breached their duty to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' Sensitive Information by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite failures and intrusions, and allowing unauthorized access to Plaintiffs' and the Class's Sensitive Information.

103. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiffs and the Class, their Sensitive Information would not have been compromised, stolen, and viewed by unauthorized persons. Defendants' negligence was a direct and legal cause of the theft of the Sensitive Information of Plaintiffs and the Class and all resulting damages. The injury and harm suffered by Plaintiffs and the Class members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and the Class members' Sensitive Information. As a result of Defendants' failure, the Sensitive Information of Plaintiffs and the Class was compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their Sensitive Information was disclosed to third parties without their consent. Plaintiffs and Class members also suffered diminution in value of their Sensitive Information in that it is now easily available to hackers on the Dark Web. Plaintiffs and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

104. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

105. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's Sensitive Information.

106. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants', of failing to use reasonable measures to protect customer information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiffs and the members of the Class's Sensitive Information.

107. Defendants breached their respective duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Sensitive Information.

108. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and its consumers, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendants were in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach.

109. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l).

Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

110. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential Sensitive Information.

111. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and the Class's Sensitive Information and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information Defendants had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

112. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class. Defendants violated their duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendants' conduct was particularly unreasonable given the nature and amount of Sensitive Information that Defendants collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

113. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiffs

and members of the Class, Plaintiffs and members of the Class would not have been injured.

114. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendants' breach of its duties. Defendants knew or should have known that Defendants were failing to meet their duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their Sensitive Information.

115. Had Plaintiffs and the Class known that Defendants did not adequately protect their Sensitive Information, Plaintiffs and members of the Class would not have entrusted Defendants with their Sensitive Information.

116. Defendants' various violations and their failure to comply with applicable laws and regulations constitutes negligence *per se*.

117. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of Sensitive Information; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Sensitive Information, entitling them to damages in an amount to be proven at trial.

118. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their Sensitive Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect their Sensitive Information in their continued possession.

COUNT III
Invasion of Privacy

(On Behalf of Plaintiffs and the Class)

119. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

120. Plaintiffs and Class Members had a legitimate expectation of privacy regarding their Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

121. Defendants owed a duty to Plaintiffs and Class Member to keep their Sensitive Information confidential.

122. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' Sensitive Information is highly offensive to a reasonable person.

123. Defendants' reckless and negligent failure to protect Plaintiffs' and Class Members' Sensitive Information constitutes an intentional interference with Plaintiffs' and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person. Defendants' failure to protect Plaintiffs' and Class Members' Sensitive Information acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

124. Defendants knowingly did not notify Plaintiffs' and Class Members in a timely fashion about the Data Breach.

125. Because Defendants failed to properly safeguard Plaintiffs' and Class Members' Sensitive Information, Defendants had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

126. As a proximate result of Defendants' acts and omissions, the private Sensitive

Information of Plaintiffs and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

127. Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Sensitive Information is still maintained by Defendants with their inadequate cybersecurity system and policies.

128. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendants' continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendants' inability to safeguard the Sensitive Information of Plaintiffs and the Class.

129. Plaintiffs, on behalf of themselves and Class Members, seek injunctive relief to enjoin Defendants from further intruding into the privacy and confidentiality of themselves and Class Members' Sensitive Information.

130. Plaintiffs, on behalf of themselves and Class Members, seeks compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

131. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

132. Plaintiffs and Class Members conferred a monetary benefit on Defendants when Defendants' clients provided Plaintiffs' and Class Members' Sensitive Information to Defendants, which Defendants collected.

133. Defendants enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Sensitive Information.

134. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and the Class, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

135. Under the principles of equity and good conscience, Defendants should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

136. Defendants acquired the monetary benefit and Sensitive Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged. If Plaintiffs and Class Members knew that Defendants had not secured their Sensitive Information, they would not have agreed to have their Sensitive Information provided to Defendants.

137. Plaintiffs and Class Members have no adequate remedy at law.

138. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to: (i) the loss of the opportunity how their Sensitive Information is used; (ii) the compromise, publication, and/or theft of their Sensitive Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Sensitive

Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Sensitive Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Sensitive Information in their continued possession and (vi) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

139. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

140. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

COUNT V
Violation of the California Confidentiality of Medical Information Act ("CMIA")
Cal. Civ. Code § 56, *et seq.*

(On Behalf of Plaintiffs and the Class)

141. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

142. Section 56.10(a) of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a

patient of the provider of health care or an enrollee or subscriber of a health care service plan without first obtaining an authorization[.]"

143. Defendants are a "contractor" within the meaning of Civil Code § 56.05(d) within the meaning of Civil Code § 56.06 and/or a "business organized for the purpose of maintaining medical information" and/or a "business that offers software or hardware to consumers . . . that is designed to maintain medical information" within the meaning of Civil Code § 56.06(a) and (b), and maintained and continues to maintain "medical information," within the meaning of Civil Code § 56.05(j), for "patients" of Defendants, within the meaning of Civil Code § 56.05(k).

144. Plaintiffs and the Class are "patients" within the meaning of Civil Code § 56.05(k). They are "endanger[ed]" within the meaning of Civil Code § 56.05(e) because Plaintiffs and the Class fear that disclosure of their medical information could subject them to harassment or abuse.

145. Plaintiffs and the respective Class members, as patients, had their individually identifiable "medical information," within the meaning of Civil Code § 56.05(j), created, maintained, preserved, and stored on Defendants' computer network at the time of the breach.

146. Defendants, through inadequate security, allowed unauthorized third-party access to Plaintiffs and each Class member's medical information, without the prior written authorization of Plaintiffs and the Class members, as required by Civil Code § 56.10 of the CMIA.

147. In violation of Civil Code § 56.10(a), Defendants disclosed Plaintiffs and the Class members' medical information without first obtaining an authorization. Plaintiffs and the Class members' medical information was viewed by unauthorized individuals as a direct and

proximate result of Defendants' violation of Civil Code § 56.10(a).

148. In violation of Civil Code § 56.10(e), Defendants further disclosed Plaintiffs and the Class members' medical information to persons or entities not engaged in providing direct health care services to Plaintiffs or the Class members or their providers of health care or health care service plans or insurers or self-insured employers.

149. Defendants violated Civil Code § 56.101 of the CMIA through their failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the Class.

150. In violation of Civil Code § 56.101(a), Defendants created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs and the Class members' medical information in a manner that failed to preserve and breached the confidentiality of the information contained therein. Plaintiffs and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendants' violation of Civil Code § 56.101(a).

151. In violation of Civil Code § 56.101(a), Defendants negligently created, maintained, preserved, stored, abandoned, destroyed, or disposed of Plaintiffs and the Class members' medical information. Plaintiffs and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendants' violation of Civil Code § 56.101(a).

152. Plaintiffs and the Class members' medical information that was the subject of the Data Breach included "electronic medical records" or "electronic health records" as referenced by Civil Code § 56.101(c) and defined by 42 U.S.C. § 17921(5).

153. In violation of Civil Code § 56.101(b)(1)(A), Defendants' electronic health record system or electronic medical record system failed to protect and preserve the integrity of

electronic medical information. Plaintiffs and the Class members' medical information was viewed by unauthorized individuals as a direct and proximate result of Defendants' violation of Civil Code §56.101(b)(1)(A).

154. Defendants violated Civil Code § 56.36 of the CMIA through their failure to maintain and preserve the confidentiality of the medical information of Plaintiffs and the Class.

155. As a result of Defendants' above-described conduct, Plaintiffs and the Class have suffered damages from the unauthorized disclosure and release of their individual identifiable "medical information" made unlawful by Civil Code §§ 56.10, 56.101, 56.36.

156. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, and violation of the CMIA, Plaintiffs and the Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory damages under the California CMIA, (v) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

157. Plaintiffs, individually and for each member of the Class, seek nominal damages of one thousand dollars ($1,000) for each violation under Civil Code § 56.36(b)(1), and actual damages suffered, if any, pursuant to Civil Code § 56.36(b)(2), injunctive relief, as well as punitive damages of up to $3,000 per Plaintiff and each Class member, and attorneys' fees,

litigation expenses and court costs, pursuant to Civil Code § 56.35.

COUNT VI
Violation of California's Consumer Records Act Cal. Bus. Code § 1798.80, *et seq.*
(On behalf of Plaintiffs and the Class)

158. Plaintiffs incorporate by reference all preceding allegations.

159. Under California law, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (CAL. CIV. CODE § 1798.2.) The disclosure must "be made in the most expedient time possible and without unreasonable delay" (*Id.*), but "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (CAL. CIV. CODE § 1798.82, subdiv. b.)

160. The data breach constitutes a "breach of the security system" of Defendants.

An unauthorized person acquired the personal, unencrypted information of Plaintiffs and the Class. Defendants knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiffs and the Class, but waited eight months to notify them. Eight months was an unreasonable delay under the circumstances.

161. Defendants' unreasonable delay prevented Plaintiffs and the Class from taking appropriate measures from protecting themselves against harm.

162. Because Plaintiffs and the Class were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

163. Plaintiffs and the Class are entitled to equitable relief and damages in an amount

to be determined at trial.

COUNT VII
Violation of California's Unfair Competition Law Cal. Bus. Code § 17200, *et seq.*
(On behalf of Plaintiffs and the Class)

164. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

165. Defendants engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, et seq. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

166. Defendants' conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, et seq. (the "CCPA"), and other state data security laws.

167. Defendants stored the PHI and PII of Plaintiffs and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiffs and the Class's PHI and PII secure and prevented the loss or misuse of that PHI and PII.

168. Defendants failed to disclose to Plaintiffs and the Class that their PHI and PII was not secure. However, Plaintiffs and the Class were entitled to assume, and did assume, that Defendants had secured their PHI and PII. At no time were Plaintiffs and the Class on notice that their PHI and PII was not secure, which Defendants had a duty to disclose.

169. Defendants also violated California Civil Code § 1798.150 by failing to employ reasonable security measures, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiffs and the Class's PHI and PII.

170. Had Defendants complied with these requirements, Plaintiffs and the Class

would not have suffered the damages related to the data breach.

171. Defendants' conduct was unlawful, in that it violated the Consumer Records Act.

172. Defendants' conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

173. Defendants' conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting PHI and PII.

174. Defendants also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that all individuals have a right of privacy in information pertaining to them. The increasing use of computers has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendants' acts and omissions thus amount to a violation of the law.

175. Instead, Defendants made the PHI and PII of Plaintiffs and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiffs and the Class to an impending risk of identity theft. Additionally, Defendants' conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

176. As a result of those unlawful and unfair business practices, Plaintiffs and the

Class suffered an injury-in-fact and have lost money or property.

177. The injuries to Plaintiffs and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

178. There were reasonably available alternatives to further Defendants' legitimate business interests, other than the misconduct alleged in this complaint.

179. Therefore, Plaintiffs and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendants; disgorgement of all profits accruing to Defendants because of their unfair and improper business practices; a permanent injunction enjoining Defendants' unlawful and unfair business activities; and any other equitable relief the Court deems proper.

PRAYER FOR RELIEF

Plaintiffs and Class Members respectfully request judgment against Defendants and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class;

D. Awarding Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

E. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Date: November 29, 2023

Respectfully submitted,

/s/ *Joe Kendall*

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
Telephone: (214)744-3000
Facsimile: (214) 744-3015
jkendall@kendalllawgroup.com

Plaintiffs' Interim Local Counsel

TURKE & STRAUSS LLP
Raina Borrelli
Samuel J. Strauss
613 Williamson Street, Suite 201
Madison, Wisconsin 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com
sam@turkestrauss.com

KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.
Melissa R. Emert
Gary S. Graifman
135 Chestnut Ridge Road
Suite 200
Montvale, NJ 07645
Telephone: (201) 391-7000
Facsimile: (201) 307-1086

memert@kgglaw.com
ggraifman@kgglaw.com

Plaintiffs' Interim Co-Lead Counsel

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
Gary M. Klinger
227 w. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
M. Anderson Berry
6200 Canoga Ave., Ste 375
Woodland Hills, CA 91367
Telephone: (916) 777-7777, ext. 238
Facsimile: (916) 924-1829
aberry@justice4you.com
Attorneys for Plaintiffs and Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing document was served on all counsel of record on November 29, 2023 via CM/ECF, in accordance with the Federal Rules of Civil Procedure.

/s/ *Joe Kendall*
JOE KENDALL